COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 9, 2001

Serial No. 107–115

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
82–173 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LaTOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee
——— ———

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
———
BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
James C. Wilson, *Chief Counsel*
Robert A. Briggs, *Chief Clerk*
Phil Schiliro, *Minority Staff Director*

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. Russell George, *Staff Director and Chief Counsel*
Elizabeth Johnston, *Professional Staff Member*
Justin Paulhamus, *Clerk*
David McMillen, *Minority Professional Staff Member*

CONTENTS

COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE?

FRIDAY, NOVEMBER 9, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL
MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representative Horn.

Staff present: Russell George, staff director and chief counsel; Bonnie Heald, deputy staff director; Elizabeth Johnston, Darren Chidsey, and Earl Pierce, professional staff members; Jim Holmes and Fred Ephraim, interns; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. HORN. The Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations is now in order. In the aftermath of the terrible events of September 11th, the Nation has prudently focused on its computer security vulnerabilities. Most of this examination has been focused on the risks to the country's physical infrastructure. However, as the oversight conducted by this subcommittee during the last 6 years has shown, the Nation cannot afford to ignore the risks associated with cyberattacks.

Federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of Americans. National defense, emergency services, tax collection, and benefit payments all rely on automated systems and electronically stored information.

Without proper protection, the vast amount of sensitive information stored on executive branch computers could be compromised and the systems themselves subject to malicious attack. As the recent spate of computer viruses and worms have shown, cyberattacks have the potential to cause great damage to the Nation.

It is imperative that the public and private leaders of this Nation know where weaknesses exist in their organizations so they can effect corrective action.

With that in mind, I am releasing an assessment of how Federal agencies rate in their computer security efforts. This is the second year that we have issued a grade on the subject. It is a disappointing feeling to announce that the executive branch of the Federal

Government has received a failing grade for its computer security efforts.

Last year Congress passed the Government Information Security Reform Act which was intended to ensure that Federal agencies establish agency-wide computer security programs that adequately protect the systems that support their missions. Based on the requirements of that law, the subcommittee has assessed the progress of 24 major executive branch departments and agencies in reaching the goals of enhanced computer security. Overall, the Federal Government received an F in this effort. The Office of Management and Budget [OMB], has set the standard. The staffs of the General Accounting Office and our subcommittee staff review the OMB inventory. Agency Inspectors General and Chief Information Officers and Chief Financial Officers have been very helpful in this.

Two thirds of the agencies failed completely in their computer security efforts: The Department of Defense, whose computers carry some of the Nation's most sensitive secrets, F. The Department of Energy, along with the Nuclear Regulatory Commission which oversees the Nation's nuclear facilities and other programs, F. The Department of Transportation, which includes the Federal Aviation Administration, an F. The Department of Health and Human Services, which holds personal information on every person who receives Medicaid and Medicare. In all, 16 Federal agencies failed this examination completely.

Five other agencies managed to keep their heads above water, but just barely. The Federal Emergency Management Agency, the General Services Administration, Environmental Protection Agency, and the Department of Housing and Urban Development at the Department of State all earned Ds.

The National Aeronautic and Space Administration did slightly better, scoring a C-minus. The Social Security Administration, which performed an admirable job of preparing for Y2K, earned only a C-plus on its computer security program. And the National Science Foundation's B-plus was the highest grade awarded this year.

All of us in Congress are well aware that the Nation is in a state of war. It is not anyone's intention to place this great land at further risk of attack. It is, however, very important that the new administration take heed of the sobering assessment the subcommittee is providing and work expeditiously to address this most important need.

[The prepared statement of Hon. Stephen Horn follows:]

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

FACSIMILE	(202) 225–3974
MAJORITY	(202) 225–5074
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

Opening Statement
Rep. Stephen Horn, R-CA
Chairman, Subcommittee on Government Efficiency,
Financial Management and Intergovernmental Relations

In the aftermath of the terrible events of September 11th, the nation has prudently focused on its vulnerabilities. Most of this examination has been focused on the risks to the country's physical infrastructure. However, as the oversight conducted by this subcommittee during the last six years has shown, the Nation cannot afford to ignore the risks associated with cyber-attacks.

Federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of Americans. National defense, emergency services, tax collection and benefit payments all rely on automated systems and electronically stored information.

Without proper protection, the vast amount of sensitive information stored on government computers could be compromised and the systems themselves subject to malicious attack. As the recent spate of computer viruses and worms have shown, cyber-attacks have the potential to cause great damage to the nation.

It is imperative that the public and private leaders of this Nation know where weaknesses exist in their organizations so that they can effect corrective action. With that in mind, the subcommittee is releasing an assessment of how Federal agencies rate in their computer security efforts.

This is the second year that the subcommittee has issued grades on this subject. It is disappointing to announce that the executive branch of the federal government has received a failing grade for its computer security efforts.

Last year Congress passed the Government Information Security Reform Act which was intended to ensure that Federal agencies establish agencywide computer security programs that adequately protect the systems that support their missions. Based on the requirements of that law, the subcommittee has assessed the progress of the 24 major executive branch departments and agencies in reaching the goals of enhanced computer security. Overall, the federal government received an "F" in this effort. The Office of Management and Budget (OMB) has set the standard. The staff of the General Accounting Office and our own subcommittee staff has reviewed the OMB inventory. Agency Inspectors General and Chief Information Officers have been helpful.

Two-thirds of the agencies failed completely in their computer security efforts.

- The Department of Defense, whose computers carry some of the nation's most sensitive secrets -- an "F."
- The Department of Energy along with the Nuclear Regulatory Commission, which oversees the nation's nuclear weapons -- another "F."
- The Department of Transportation, which includes Federal Aviation Administration -- an "F."
- The Department of Health and Human Services, which holds personal information on every person who receives Medicare or Medicaid -- "F."

In all, 16 federal agencies failed this examination completely.

Five other agencies managed to keep their heads above water -- but just barely. The Federal Emergency Management Agency, General Services Administration, Environmental Protection Agency, and the Department of Housing and Urban Development, and Department of State all earned "D's."

The National Aeronautics and Space Administration did slightly better, scoring a "C-minus." The Social Security Administration, which performed an admirable job of preparing for Y2K, earned only a "C-plus" on its computer security program. And the National Science Foundation's "B-plus" was the highest grade awarded this year.

All of us in Congress are well aware that the nation is in a state of war. It is not anyone's intention to place this great land at further risk of attack. It is, however, very important that the new administration take heed of the sobering assessment the subcommittee is providing and work expeditiously to address this most important need.

I welcome our witnesses today, and look forward to their testimony.

Mr. HORN. And we have two excellent witnesses today, and that is Robert F. Dacey, Director, Information Security, U.S. General Accounting Office. We also have Mark A. Forman, Associate Director, Information Technology and E-Government, Office of Management and Budget.

Gentlemen, as you know, we swear in witnesses here and your staff that have accompanied you, and the clerk will keep tabs of who the staff are and so forth and put it in the hearing record. So if you will stand and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note that we have six witnesses and supporters.

And our first witness is Robert Dacey, the Director, Information Security U.S. General Accounting Office. Welcome.

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY, U.S. GENERAL ACCOUNTING OFFICE

Mr. DACEY. Thank you. Mr. Chairman, I am pleased to be here today to discuss our recent analysis of information security audits and evaluations of unclassified computer systems at 24 major departments and agencies. As you requested, I will briefly summarize my written statement.

Overall, the audit shows that significant pervasive computer security weaknesses continue to place Federal assets and operations at risk. As with other large organizations, Federal agencies rely extensively on computerized systems and electronic data to support their missions. If these systems are inadequately protected, resources such as Federal payments and collections could be lost or stolen. Computer resources could be used for unauthorized purposes or to launch attacks on others.

Sensitive information such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed or browsed or copied for purposes of espionage or other crimes. Critical operations such as those supporting national defense and emergency services could be disrupted. Data could be modified or destroyed for purposes of fraud, deception or disruption, and agency missions could be undermined by embarrassing incidents that result in diminished confidence in the Federal Government's ability to conduct its business in a secure manner.

Further, these risks are rapidly increasing. Greater complexity and interconnectivity of systems including Internet access are providing additional potential avenues for cyberattack.

Second, more standardization of systems hardware and software is increasing the exposure to commonly known vulnerabilities.

Third, the increased volume, sophistication and effectiveness of cyberattacks, combined with readily available intrusion, or hacking tools, and limited capabilities to detect cyberattacks.

And, fourth, other nations, terrorists, transnational criminals, and intelligence services are developing cyberattack capabilities. The threat of cyberattacks can also arise from hackers and others. For example, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets.

Given these risks, I would like to turn to the status of Federal agency information security. Our most recent analysis of reports published from July 2000 to September 2001 continue to show significant weaknesses in Federal unclassified computer systems that put critical operations and assets at risk.

We have reported the potentially devastating consequences of poor information security since September 1996 and have identified information security as a governmentwide high-risk area since 1997, and most recently in January 2001. As the body of audit evidence continues to expand, it is probable that additional significant deficiencies will be identified.

Weaknesses continue to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls which are those policies, procedures, and technical controls that apply to all or most of computer processing and help ensure their proper operation.

This chart illustrates the distribution of weaknesses for the six general control areas across the 24 agencies. As we have reported in the past, information security problems persist in a large part because agency managers have not yet established comprehensive security management programs.

As further evidence of vulnerabilities, the Inspectors General reported significant deficiencies in agency-critical infrastructure protection efforts. During the past 2 years, a number of improvement efforts have been initiated. For example, several agencies have taken significant steps to redesign and strengthen their information security programs. In addition, the Federal Chief Information Officer or CIO Council has issued a guide for measuring agency progress which we assisted in developing. And the President issued a national plan for information systems protection in January 2000.

More recently, partially in response to the events of September 11th, the President created the Office of Homeland Security with duties that include coordinating efforts to protect public and private information systems in the United States from terrorist attack. The President also appointed a special advisor for cyberspace security to coordinate interagency efforts to secure information systems and created the President's Critical Infrastructure Protection Board to recommend policies and coordinate programs for protecting critical infrastructure. The Board is to include a standing committee for executive branch information systems security, which is to be chaired by an OMB designee.

These actions are laudable. However, given recent events and the reports that critical assets and operations continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyberthreats are appropriately addressed in the context of the broader array of risks to the Nation's welfare.

Accordingly, it is important that Federal information security be guided by a comprehensive strategy for improvement. As the administration refines its strategy that it has begun to lay down in recent months, it is imperative that it take steps to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed.

First, it is important that Federal strategy delineate the roles and responsibilities of the numerous entities involved in Federal information security and the related aspects of critical infrastructure protection. Further, there is a need to clarify how these activities of these many organizations interrelate, who should be held accountable for the success and failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on controls that they need to implement could help to ensure adequate protection. Currently agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls.

Third, there is a need for effective agency monitoring to determine if milestones are being met and testing to determine if policies and procedures are operating as intended. Routine periodic audits such as those required in recent government information security reform legislation would allow for more meaningful performance measurement.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls to protect their systems. Similarly, the Federal Government must maximize the value of its technical staff by sharing expertise and information.

Sixth, agencies can allocate resources sufficient to support their computer security and infrastructure protection activities. Some additional amounts are likely to be needed to address significant weaknesses and new tasks. OMB and congressional oversight for future spending on computer security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc piecemeal security fixes that are not supported by strong agency risk management process.

And, last, expanded research is needed in the area of information security protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances.

Mr. Chairman, this concludes my statement. I will be pleased to answer any questions that you have at this time.

Mr. HORN. Well, thank you Mr. Dacey.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EST
Friday,
November 9, 2001

COMPUTER SECURITY

Improvements Needed to Reduce Risk to Critical Federal Operations and Assets

Statement of Robert F. Dacey
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analysis of recent information security audits and evaluations at federal agencies. As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information.

Our analyses covers information security audits and evaluations that we and agency inspectors general (IGs) performed since July 2000 at 24 major federal departments and agencies. In summarizing these results, I will discuss the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997. I will then illustrate the serious risks that these weaknesses pose at selected individual agencies and also describe the major common weaknesses that agencies need to address to improve their information security programs. Finally, I will discuss the importance of establishing a strong agencywide security management program in each agency and developing a comprehensive governmentwide strategy for improvement.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with virtually an unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Reports of attacks and disruptions are growing. The number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 21,756 in 2000 and 34,754 for just the first 9 months of 2001.[1] And these are only the *reported* attacks. The CERT® Coordination Center estimates that as much as 80 percent of actual security incidents go unreported, in most cases because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack. As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A potential hacker can literally download tools from the Internet and "point and click" to start a hack. According to a recent National Institute of Standards and Technology (NIST) publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month.

Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Attacks over the past several months illustrate the risks. As we reported to this Subcommittee in August 2001, the attacks referred to as Code Red, Code Red II, and SirCam have affected millions of computer users, shut down web sites, slowed Internet service, and disrupted business and government operations, and have reportedly caused billions of dollars in damage.[2] More recently, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus, allowing it to spread widely in a short amount of time.[3]

As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood that information attacks will threaten vital national interests increases. Government officials have

[1] CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[2] *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

[3] *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.

long been concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, worms, Trojan horses, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data.[4] In addition, the disgruntled organization insider is a significant threat, since such individuals with little knowledge about computer intrusions often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets. Examples of such attacks already exist:

- In October 2000, the FBI's National Infrastructure Protection Center (NIPC) issued an advisory concerning an increased level of cyber activity against web sites related to Israel and pro-Palestinian organizations. This advisory noted that due to the credible threat of terrorist acts in the Middle East region, and the conduct of these web attacks, increased vigilance should be exercised to the possibility that U.S.-government and private-sector web sites may become potential targets. In less than a month, a group of hackers calling itself Gforce Pakistan defaced more than 20 web sites and posted threats to launch an Internet attack against AT&T. Further, in October 2001, this same group attacked a government web server operated by the National Oceanic and Atmospheric Administration, defacing a web site and threatening to release some highly confidential data unless the United States met several demands.

- According to recent Defense Intelligence Agency and Central Intelligence Agency estimates, at least 20 countries are known to be developing information warfare strategies that specifically target U.S. military and private-sector data networks. The fear is that computer viruses and worms unleashed by foreign hackers could wreak havoc on the U.S. infrastructure in the event of a military conflict.

- In his April 2001 written statement for the House Energy and Commerce Committee on intrusions into government computer networks, the director of the NIPC noted that terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely.[5] Citing the example of convicted terrorist Ramzi

[4] *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

[5] "Issue of Intrusions into Government Computer Networks," Statement for the Record by Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the House Energy and Commerce Committee, Oversight and Investigation Subcommittee, April 5, 2001.

Yousef, who masterminded the 1993 World Trade Center bombing and stored detailed plans to destroy U.S. airliners in encrypted files on his laptop computer, the director concluded that while we have not yet seen terrorist groups employ cyber tools as a weapon against critical infrastructures, the reliance of these groups on information technology and acquisition of computer expertise are clear warning signs.

After the September 11, 2001, attacks, the NIPC warned of an expected upswing in incidents and encouraged system administrators to follow best practices to limit the potential damage from any cyber attacks. In particular, it warned that political events and international situations would likely lead to increasing cyber protests and that such attacks were expected to now target the information infrastructure more often and exploit opportunities to disrupt or damage it. On November 2, the NIPC updated its warning, noting that hacking groups have formed and participated in pro-U.S. and anti-U.S. cyber activities, which have mainly taken the form of web defacements. The NIPC went on to say that while there has been minimal activity in the form of denial-of-service attacks, it has reason to believe that the potential for such attacks in the future is high and that infrastructure support systems must take a defensive posture and remain at a higher state of alert.

Finally, while the warning of a potential "digital Pearl Harbor" has been raised in the past, the events of September 11, 2001, further underscored the need to protect America's cyberspace against potentially disastrous cyber attacks. In his September 2001 testimony before this Subcommittee on cyber attacks, the former NIPC Director warned that a cyber attack by terrorists or nation-states using multiple-attack scenarios could have disastrous effects on infrastructure systems and could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both. Further, in his October congressional testimony, Governor James Gilmore, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, cautioned that our critical information and communication infrastructures are targets for terrorists because of the broad economic and operational consequences of a shutdown.[6] He warned that systems and services critical to the American economy and the health of our citizens—such as banking and finance, "just-in-time" delivery system for goods, hospitals, and state and local emergency services—can all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.

[6] Testimony of Governor James S. Gilmore, III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the House Science Committee, October 17, 2001.

Weaknesses in Federal Systems Remain Pervasive

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[7] Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 agencies had significant information security weaknesses.[8] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[9]

Our most recent analyses, of reports published from July 2000 through September 2001, continue to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[10] Weaknesses continued to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 1 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

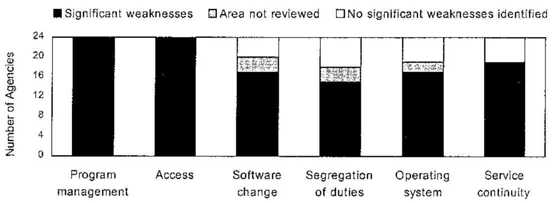
[7] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

[8] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[9] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); High-Risk Series: An Update (GAO/HR-99-1, January 1999); *High Risk Series: An Update* (GAO-01-263, January 2001).

[10] These reports include the independent IG evaluations of agencies' information security programs required by the Government Information Security Reform provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398).

Figure 1: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued July 2000 through September 2001

As in 2000, our current analysis shows that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively. For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

In 2001, we also found weaknesses at 19 of the 24 agencies (79 percent) for service continuity controls (compared to 20 agencies or 83 percent in 2000). These controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 1 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue.

Audit coverage for nonfinancial systems is also likely to increase as agencies review and evaluate their information security programs as required by government information security reform provisions.[11] These provisions require agencies to implement security program management improvements, perform annual management reviews, have independent IG evaluations of agencies' information security programs, and report the results of these reviews and evaluations to the Office of Management and Budget (OMB). As I will discuss later in my testimony, the first reports under these new provisions were submitted to OMB in September 2001.

Information security weaknesses are also indicated by the limited agency progress in implementing Presidential Decision Directive (PDD) 63 to protect our nation's critical infrastructures from computer-based attacks.[12] A March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in agencies' implementation of PDD 63 based on reviews conducted by agency IGs.[13]

[11] P.L. 106-398.

[12] Issued in May 1998, Presidential Decision Directive (PDD) 63 called for a range of activities to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious attacks. The directive established critical infrastructure protection as a national goal, stating that, by the close of 2000, the United States was to have achieved an initial operating capability and, no later than 2003, the capability to protect the nation's critical infrastructures from intentional destructive acts.

[13] The PCIE primarily comprises the presidentially appointed IGs and the ECIE primarily comprises the agency head-appointed IGs. In November 1999, PCIE and ECIE formed a working group to

This report concluded that the federal government could improve its PDD 63 planning and assessment activities and questioned the federal government's ability to protect the nation's critical infrastructures from intentional destructive acts by May 2003, as required in PDD 63. Specifically, the report stated that

- many agency critical infrastructure protection plans were incomplete, and some agencies had not developed such plans,
- most agencies had not completely identified their mission-essential infrastructure assets, and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective IG reviews.[14] For example, while five agencies had or were in the process of updating their plans, three were not revising their plans to address reported deficiencies. In addition, while most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the eight agencies we reviewed had not taken the additional steps to identify interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. Identifying interdependencies is important so that infrastructure owners can determine when disruption in one infrastructure could result in damage to other infrastructures.

Substantial Risks Persist for Federal Operations, Assets, and Confidentiality

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 IGs of their respective agencies' PDD 63 planning and assessment activities.

[14] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

More recent audits in 2001 show that serious weaknesses continue to be a problem and that critical federal operations and assets remain at risk:

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[15] Commerce's IG has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[16]

[15] *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* (GAO-01-751, August 13, 2001).

[16] *Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements*, Inspector General Audit Report No. FSD-12849-1-0001.

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[17]

- In March, we reported that although the Department of Defense's (DOD's) Departmentwide Information Assurance Program made progress, it had not yet met its goals of integrating information assurance with mission-readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[18]

- In February, the Department of Health and Human Services' IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[19] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which, during fiscal year 2000, was responsible for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data (such as Medicare enrollment, eligibility, and paid claims data) and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

To correct reported weaknesses, several agencies took significant steps to redesign and strengthen their information security programs. For example, IRS made notable progress in improving computer security at its facilities, corrected a significant number of identified weaknesses, and established a servicewide computer security management program that, when fully implemented, should help

[17] *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* (GAO-01-615, July 3, 2001).

[18] *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, March 30, 2001).

[19] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000*, A-17-00-00014, February 26, 2001.

the agency effectively manage its security risks.[20] Similarly, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we identified in February 2000.[21] While we have not tested their effectiveness, these actions show that the agency is taking a comprehensive and systematic approach that should help ensure that its efforts are effective.

Also, the types of risks I have described, if inadequately addressed, may limit the government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits.

Specifically, we found that during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both within and outside IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electronic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS completed corrective action for all the critical access control vulnerabilities we identified before the 2001 filing season and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[22]

Addressing weaknesses such as those we identified in the IRS' electronic filing system is especially important in light of the administration's plans to improve government services by expanding use of the Internet and other computer-facilitated operations—collectively referred to as electronic government, or E-government.[23] Specific initiatives proposed for fiscal year 2002 include expanding electronic means for (1) providing information to citizens, (2) handling procurement-related transactions, (3) applying for and managing federal grants, and (4) providing citizens information on the development of specific federal rules and regulations. Anticipated benefits include reducing the expense and difficulty of

[20] *Financial Audit: IRS' Fiscal Year 1999 Financial Statements* (GAO/AIMD-00-76, February 29, 2000).

[21] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

[22] Information Security: IRS Electronic Filing Systems (GAO-01-306, February 16, 2001).

[23] The President's Management Agenda, Fiscal Year 2002, www.whitehouse.gov/omb/budget.

doing business with the government, providing citizens improved access to government services, and making government more transparent and accountable. Success in achieving these benefits will require agencies and others involved to ensure that the systems supporting E-government are protected from fraud, inappropriate disclosures, and disruption. Without this protection, confidence in E-government may be diminished, and the related benefits never fully achieved.

Similar Control Weaknesses Continue Across Agencies

Although the nature of agency operations and their related risks vary, striking similarities remain in the specific types of general control weaknesses reported and in their serious adverse impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions agencies must take. The following sections describe the six areas of general controls and the specific weaknesses that have been most widespread at the agencies covered by our analyses.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost-effective manner rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk, (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,

- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they execute. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Also, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and departing employees, as well as changes in users' responsibilities and related access needs.

Significant access control weaknesses that we have commonly identified include the following:

- Accounts and passwords for individuals no longer associated with an agency are not deleted or disabled or are not adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, in some cases, former employees and contractors could still and in many cases did read, modify, copy, or delete data; and even after long periods of inactivity, many users' accounts had not been deactivated.
- Users are not required to periodically change their passwords.

- Managers do not precisely identify and document access needs for individual users or groups of users. Instead, they provide overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. For example, in some cases, large numbers of users were granted access to sensitive system directories and settings or provided access to systems without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increases the risk of unauthorized access. We are often able to guess many passwords based on our knowledge of commonly used passwords and to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.

- Software access controls are improperly implemented, resulting in unintended access or gaps in access-control coverage. For example, in some cases, excessive numbers of users, including programmers and computer operators, had the ability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. In addition, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate network vulnerability testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. In almost every test, our auditors have been successful in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Much of the activity associated with our intrusion testing had not been recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and different versions are not misidentified.

Such controls can prevent errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that, depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Examples of weaknesses in this area included the following:

- Testing procedures are undisciplined and do not ensure that implemented software operates as intended. For example, systems were sometimes authorized for processing without testing access controls to ensure that they had been implemented and were operating effectively. Also, documentation was not always retained to demonstrate user testing and acceptance.
- Implementation procedures do not ensure that only authorized software is used. In particular, procedures do not ensure that emergency changes are subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs is prevented or detected.
- Agencies' policies and procedures frequently do not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or

- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. Common problems involve computer programmers and operators who are authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. An example of this would be a single individual authorized to independently develop, test, review, and approve software changes for implementation.

We also identify segregation-of-duties problems related to transaction processing. For example, we found staff members involved with procurement that had system access privileges allowing them to individually request, approve, and record the receipt of purchased items. In addition, we found staff members with system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes.

Operating System Software Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that security controls over operating system are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues previously discussed. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. A common type of problem reported is insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, we found system support personnel that had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Further, pervasive vulnerabilities in network configuration expose agency systems to attack. These vulnerabilities stem from agencies' failure to (1) install and maintain effective perimeter security, such as firewalls and screening routers, (2) implement current software patches, and (3) protect against commonly known methods of attack.

Service Continuity Controls

Finally, the terrorist events that began on September 11, 2001, have redefined the disasters that must be considered in identifying and implementing service continuity controls to ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.

To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. Agencies should then take steps to prevent and minimize potential damage and interruption. These steps include routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage; installing environmental controls, such as fire suppression systems or backup power supplies; arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and ensuring that staff and other users of the system understand their responsibilities in case of emergencies. Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location[24] and travel and lodging for necessary personnel, off-site storage location for backup files, and

[24] Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors, such as making arrangements with suppliers of computer hardware and telecommunications services, as well as with suppliers of business forms and other office supplies.

procedures for restoring critical applications and their order in the restoration process. In testing the plan, it is most useful to simulate a disaster situation that tests overall service continuity, including whether the alternative data processing site functions as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Such testing not only helps managers identify weaknesses, it also assesses how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.

Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. As we reported in September 2000 on the lessons learned from this challenge, developing these plans was one of a number of management practices that, if continued, could improve federal agencies' overall information technology management, particularly in areas such as critical infrastructure protection and security.[25]

In the aftermath of the September 11, 2001, attacks, news reports indicate that business continuity and contingency planning has been a critical factor in restoring operations for New York's financial district, with some specifically attributing companies' preparedness to the contingency planning efforts begun for the Year 2000 challenge. In particular, the Year 2000 challenge increased management attention on continuity and risk management. It also gave companies a chance to rehearse a disaster beforehand. However, whereas the Year 2000 challenge may have increased the focus on business continuity and contingency planning, our analyses show that most federal agencies currently have service continuity control weaknesses. Examples of common agency weaknesses include the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.

[25] *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges* (GAO/AIMD-00-290, September 12, 2000).

- Disaster recovery plans were not fully tested to identify their weaknesses. For example, agencies had not performed periodic walkthroughs or unannounced tests of the disaster recovery plan—tests that provide a scenario more likely to be encountered in the event of an actual disaster.

Agencies Can Take Immediate Steps to Improve Security Program Management

Our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. Agencies have taken steps to address problems, and many have remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management program.

Establishing such a management program requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments.

Implementing this cycle of risk management activities is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, agencywide basis. Included within it are several steps that agencies can take immediately. Specifically, agencies can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. Although none of these actions alone will ensure good security, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, these are steps that can be made without delay.

Improvement Efforts Are Underway, But Challenges Remain

During the last 2 years, a number of improvement efforts have been initiated. As mentioned previously, several agencies have taken significant steps to redesign and strengthen their information security programs. In addition, the Federal Chief Information Officers (CIO) Council has issued a guide for measuring agency progress, which we assisted in developing, and the President issued a National Plan for Information Systems Protection in January 2000.

More recently, partially in response to the events of September 11, 2001, the President created the Office of Homeland Security with duties that include coordinating efforts to protect critical public and private information systems within the United States from terrorist attack. The President also appointed a Special Advisor for Cyberspace Security to coordinate interagency efforts to secure information systems and created the President's Critical Infrastructure Protection Board to recommend policies and coordinate programs for protecting information for critical infrastructure. The Board is to include a standing committee for executive branch information systems security, chaired by an OMB designee.

These actions are laudable. However, recent reports and events indicate that these efforts are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks. The government faces a challenge in ensuring that risks from cyber threats are appropriately addressed in the context of the broader array of risks to the nation's welfare that have recently been demonstrated.

Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement. In 1998, shortly after the initial issuance of PDD 63, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs work together to ensure that the roles of new and existing federal efforts were coordinated under a comprehensive strategy.[26] Our more recent reviews of the NIPC and of broader federal efforts to counter computer-based attacks showed that there was a continuing need to clarify responsibilities and critical infrastructure protection objectives.[27] As the administration refines the strategy that it has begun to lay out in recent months, it is imperative that information security receives appropriate attention and resources and that known deficiencies are addressed. Specific steps in this process are outlined below.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security, and NIST, with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies—such as the CIO Council and the entities created under Presidential Decision Directive 63 on critical infrastructure protection—are attempting to coordinate agency initiatives. Although these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not taking place. It is unclear how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data.

Our studies of best practices at leading organizations have shown that more specific guidance is important. In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; and help ensure that shared data are appropriately protected. Implementing such standards for federal agencies would require developing a single set of

[26] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[27] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001); *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required in the government information security reforms recently enacted, would allow for more meanii.gful performance measurement. Agencies and the IGs have completed their first agency reviews and independent evaluations as required by this legislation and submitted their results to OMB. In addition, agencies are also to submit plans of action and milestones for correcting their information security weaknesses. This annual evaluation, reporting, and monitoring process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and for managing the problem from a governmentwide perspective.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, of importance is that agencies have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As the Year 2000 challenge showed, the availability of adequate technical expertise has been a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their computer security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on computer security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As the Director of the CERT® Coordination Center testified before this subcommittee last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in the October 31 advance executive summary of its forthcoming third report, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (commonly known as the "Gilmore Commission") recommended that the President establish a comprehensive plan of research, development, test, and evaluation to enhance cyber security.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

Contact

If you should have any questions about the testimony, please contact me at (202) 512-3317. I can be reached by e-mail at daceyr@gao.gov.

(310137)

Mr. HORN. We now go to Mark A. Forman, Associate Director, Information Technology and E-Government, Office of Management and Budget. Welcome here.

STATEMENT OF MARK A. FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET

Mr. FORMAN. Thank you, Mr. Chairman. Thank you for inviting me here to discuss the administration's efforts in the areas of computer security. Before getting to the substance of my testimony, I would like to commend you and the committee for your past and current efforts to shine the spotlight on Federal agency security performance. I believe that only by keeping the pressure on this issue will we get the improved performance, will we be able to achieve and sustain the targets that we are all searching for achieving.

As you know, the President's given a high priority to the security of government assets including information systems and the protection of our Nation's critical information assets. The President has taken a number of steps to address these risks. Last month the President signed Executive Order 13228 which established the Office of Homeland Security and the Homeland Security Council.

The Executive order provides for the implementation of a comprehensive national strategy for detecting, preparing for, preventing, protecting against, responding to and recovering from terrorist threats and attacks within the United States to work with Governor Ridge on issues related specifically to the topic of today's hearing—that is, the security of information systems—the President appointed Richard Clarke as Special Advisor for Cyberspace Security and issued Executive Order 13231, "Critical Infrastructure Protection in the Information Age."

The President has made OMB a member of both the Homeland Security Council and the Critical Critical Infrastructure Protection Board. We will help identify resource shortfalls and duplication and ensure that funding requests are included in the President's budget, as necessary, and properly managed when appropriated by Congress.

OMB's presence on both organizations also reflects our statutory role regarding the security of Federal information systems. Now, over the last 3 years, Congress has passed two laws that have helped to shape our current efforts in security. In 1998 the Government Paperwork Elimination Act, GPEA was passed. GPEA addressed OMB and agency responsibilities for conducting business in an electronic environment and recognized that improved government performance demands an ability to broadly accept authenticated electronic business transactions. Last year, through passage of the Government Information Security Reform Act, which we will refer to as the "Security Act," Congress strengthened the legal framework for the executive branch to address computer security needs.

Working within this legal framework, OMB is to continuously improve Federal security programs. Our guidance ensures that agency senior managers devote greater attention to security; requires agencies to tie security to their capital planning and investment control process and to their budget as required under the Clinger-Cohen Act, the Security Act, and indeed by our policy. It helps agencies get user buy-in for security control and processes to ensure that they enable business operations. It requires that security is part of agency program management. And it makes adequate security a condition for funding by requiring that security controls and their costs be explicitly identified.

The agencies have reported that for fiscal year 2002 they are investing approximately $2.7 billion for security and critical infrastructure protection. Of course, there are embedded security elements such as software and protocols within our overall IT spending. So this is buried within a total information technology budget for 2002 of approximately $45 billion.

But a high dollar figure says little about effective security. In fact, we have done some analysis on our evaluation of the 2002 reports and we found there is no significant relationship between the percent of IT spending on security to the security performance of that agency.

Now, as you know, several of your ratings, based on our staff discussions, are a little tougher than ours. Some of yours are a little lenient. If we were to add in your ratings though, I have no doubt that would show a negative relationship between IT spending and their security performance. So——

Mr. HORN. Let me just ask for a fact here, to get it in the record. Is that figure you gave us $2 billion, was that it?

Mr. FORMAN. $2.7 billion.

Mr. HORN. $2.7. Does that include the intelligence hardware, software?

Mr. FORMAN. It would for the Defense Department, but not for Intelligence Community spending.

Mr. HORN. OK. Because I think some of that needs to be carved out before we look at the 24 agencies, minus one or two. Go ahead.

Mr. FORMAN. In essence, we don't believe that simply adding more money will solve the problems. It has not worked for IT in general. It shifts attention away from effective management and investment of existing resources, and we don't believe it will work for IT security.

To ensure that security is addressed both in apportionment of the 2002 agency funds and in their 2003 budget request, we have established four criteria: First, agencies must report their security costs for each measure and significant IT systems. Systems that fail to document their security costs will not be funded.

Second, agencies must document in their capital asset plans that adequate security controls have been incorporated into the lifecycle planning and funding for each system.

Third, agency security reports and corrective action plans are presumed to reflect agencies' security priorities and thus are a central tool that we are using in prioritizing funding for systems at the agencies.

And, four, agencies must tie their corrective action plans for a system directly to the capital asset plan for that system, thereby establishing the audit trail that we know that the actions are underway.

In September we began to receive the agency reports as required by the Security Act. We are reviewing them now because we know that there will be much consultation with the agencies regarding their submissions. It is too early to make public our specific findings regarding any particular agency. I will point out at this point that we do see the Defense Department is operating a significantly higher level of performance in security than your ratings would suggest. But later I will provide you some broad observations.

First I want to talk about our process and how we have gone significantly further than the law requires insofar as reporting and follow-up. As you know, the Security Act's reporting requirements are relatively narrow, requiring only that the agency Inspectors General submit an annual independent evaluation to OMB. But because security is a high priority for this administration, we have expanded the Security Act's reporting requirements. We have issued guidance throughout the year on meeting these requirements, including detailed instructions to agencies on how to report the results in an executive summary. To ensure that reporting does not devolve into a paper drill, we are also requiring that agencies produce for their own use and send to us copies of corrective action plans and milestones for each weakness found by an IG evaluation, a program review, or any other review conducted throughout the year including GAO audits. These plans bring a discipline to the process and make tracking progress much easier for all involved.

We will also seek brief quarterly certifications that corrective actions are on track. We intend to use the security reports from the agencies, the information we have gathered from meetings with the agencies on integrating security into their capital planning process and in budget submissions with other sources to determine whether OMB must take steps to assist agencies in quickly correcting the most serious weaknesses.

In general, based on the security reports, we found across the 24 CIO agencies that the most common problems involved inadequate compliance with existing OMB security policies and a failure to follow the implementing guidance for the Security Act.

Based on our preliminary findings, agencies have to do a better job testing and evaluating the basic security controls; improve the ongoing maintenance of system security; greatly improve employee training and awareness programs; do a better job integrating security into their capital planning and budgeting process; recognize greatly increased risk of interconnection; require that every system supporting operations and their assets are reviewed annually as part of the program review; install readily available patches for commonly known vulnerabilities. As you know this is a chronic problem identified by GAO, the IGs, and most any security program in view.

It's also commonly reported from FedCIRC and others as the cause of some 90 percent of the successful attacks on the agency. This list represents what I would call the blocking and tackling, and not the policy gaps, but the details of what needs to be done in the agencies.

The reporting requirements of the Security Act have given us a starting point to measure the performance, a baseline. And this is our first opportunity to analyze the comprehensive information from agencies, and from this we can move forward on resolving the security concerns.

I would also like to take a moment to update you on two other security-related initiatives we are working on. The first involves our E-Government initiatives. We are currently working with agencies on a number of high-payoff, cross-agency E-Government initiatives. All of these initiatives will address security within their business cases as we're requiring a detailed business case be made for each of them.

Additionally, we have three specific initiatives that deal with security issues.

First, E-authentication, ensuring that parties to a transaction are authorized to participate, and it would ensure the integrity of the transaction.

Second, the wireless networks initiative, ensuring effective and interoperable communications between public safety officials throughout all levels of government, Federal, State and local, before, during and after the response to an emergency.

And, third, disaster assistance and crisis response, providing a one-stop portal containing information from all public and private organizations involved in disaster preparedness response and recovery.

A second major issue on another front is that we are directing large agencies under a Project Matrix view. Project Matrix identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships within that agency and beyond into the enterprise architecture. Fiscal year 2002 funds will be re-allocated to provide for Matrix review. Once the reviews have been completed at each large agency, OMB will identify cross-government activities and the associated lines of business. In this way, we will have identified both the vertical and the horizontal critical operations; in other words, within an agency or department and between agencies and department, and the assets and the relationships beyond government; in essence the government's critical enterprise architecture.

I'd just like to sum up with a few comments. We are planning to engage the agencies in a number of ways to address the problems that have been identified. We are going to be emphasizing both the responsibilities and the performance of agency employees, in addition to accountability for exercising those responsibilities, and consequences for poor performance. At the same time, we are going to focus on achieving sustained senior management attention at the agencies. In the past this has been a chronic problem that we at GAO and others have found over the years to be the underlying cause for poor security performance.

And, Mr. Chairman, as you know, I worked for many years on the Senate Governmental Affairs Committee. Computer Security Act oversight was part of my portfolio. And we have a chronic issue of getting department secretaries and agency heads to focus on this. I am quite pleased this year that in the agency it gives a report, it is a Security Act report. We had many agency heads and secretaries signing-off on the report. So I am pleased that we are finally starting to get the senior executive view in this important issue.

In discharging our responsibilities under the Security Act, the director will be communicating with the appropriate agency heads to impress upon them the true improvement in security performance that has to come out of external oversight from OMB, the IGs and GAO. Congressional committee is insufficient. It's got to come from within the agencies. So we're impressing upon them the importance of holding agency employees, including the CIOs and program officials, accountable for fulfilling their responsibilities under the Security Act. There have to be consequences for inadequate performance. We will also underscore an essential companion to that accountability, the clear and unambiguous authority to exercise those responsibilities.

Again, I want to thank you and the committee for your help and continued focus on this important area. It's vital that we all work together to maintain this as a priority issue, and thus promote a more secure government. Thank you.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES
November 9, 2001

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss the Administration's efforts in the areas of computer security. We know that our government and our nation rely increasingly on computer systems to support nearly every critical governmental and business function.

Government and industry are now more interconnected than ever, operating in a shared risk environment, with our interdependence growing daily. The integrity and availability of our systems and, where appropriate, the confidentiality and privacy of information in those systems are today more important than ever. The value of computer and telecommunications systems and the vital information they process and transport became even more apparent in the wake of the tragic events of September 11.

I would like to commend you and the Committee for your past and current efforts to shine the spotlight on Federal agency security performance. I believe that only by keeping the pressure on will improved performance be achieved and sustained.

Before I get to the substance of my testimony, I need to make sure the Subcommittee understands that I do not serve in a confirmed position within the Office of Management and Budget (OMB). As a general policy, OMB does not usually send officials in non-confirmed political positions to testify before Congress. However, in this case, because OMB does not yet have a Deputy Director for Management, the OMB Director decided it was in the best interest of the Administration to have me appear on his behalf as a witness for this hearing.

Setting the Context

The President has given a high priority to security of government assets including government information systems and to the protection of our nation's critical information assets. In addition to the real risk to our physical well being, he understands the growing risks that our nation faces from cyber threats and of course the risks to our cyber assets that physical attacks can bring.

At the same time we know that interconnected computer systems are necessary for the provision of essential national services. Government and industry face the same risks and must work in close partnership to mitigate those risks. Indeed, this risk is also shared globally.

The President has taken a number of steps to address these risks. First, on October 8, 2001, the President signed Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council" which provides for the implementation of a comprehensive national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats and attacks within the United States. As you know, the President appointed Governor Tom Ridge to head this office. The Governor and his staff are working hard to set the framework for this complex undertaking and the President recently convened the Homeland Security Council to help this process.

To work with Governor Ridge on issues related specifically to the topic of today's hearing -- the security of information systems -- the President appointed Richard Clarke as the Special Advisor to the President for Cyberspace Security. Mr. Clarke will be leading the Administration's cyberspace security efforts under the guidelines established in Executive Order 13231,"Critical Infrastructure Protection in the Information Age." Under this executive order, Mr. Clarke will chair the Critical Infrastructure Protection Board to promote greater coordination and consistency among the Federal agencies and ensure that Federal policies and processes are adequate to ensure information technology assets are adequately secure, that emergency preparedness communications are operating adequately, and that government and industry work closely together to address their ever increasing interconnections and shared risk.

The President has made OMB a member of both the Homeland Security Council and the Critical Infrastructure Protection Board to help identify resource shortfalls and duplication and ensure that funding requests are included in the President's budget as necessary and properly managed when appropriated by Congress.

OMB's presence on both organizations also reflects OMB's statutory role regarding the security of Federal information systems.

Among the issues that the Office of Homeland Security and the Critical Infrastructure Protection Board will focus on is the relationship between the government's programs for security, critical infrastructure protection, and continuity of government operations. In most respects these are related and complementary programs and effective implementation of one program helps promote effective implementation of the other two. At the same time, we want to remove any duplication of effort and find any wasteful expenditure of scarce resources so that collectively these programs can operate more effectively and be funded adequately.

The Legal Framework for Government Computer Security

In 1998 the Government Paperwork Elimination Act (GPEA) addressed OMB and agency responsibilities for conducting business in an electronic environment. The authors of GPEA had the foresight to recognize that improved government performance demands an ability to broadly accept authenticated electronic business transactions. Fulfilling this goal is essential to achieving the President's Management Agenda. We are now reviewing updated plans from the agencies to evaluate whether they are on track to meet the October 2003 GPEA deadline.

Last year, through passage of the Government Information Security Reform Act of 2000 (Security Act), Congress strengthened an already sound legal framework for the Executive branch to address computer security needs.

The Security Act amends the Paperwork Reduction Act of 1995 (PRA) by adding a new subchapter on Information Security and builds upon the Computer Security Act of 1987 and the Information Technology Reform Act of 1996 (Clinger-Cohen). Like the PRA itself and Clinger-Cohen, the Security Act binds agency security programs and practices to their overall program and information resource management and capital planning and budget processes.

The Security Act divides security programs into three basic components -- management, implementation, and evaluation.

-- For management, it recognizes that while security has a technical component, it is at its core, an essential management function.

-- For implementation, it recognizes that program officials (not security officers or CIOs) are ultimately responsible for ensuring that security is integrated and funded within their programs and tied to the program goals.

Thus the Security Act highlights the reality that when security funding and implementation are separated from the operational program, program officials and users begin to ignore it. Separation sends the incorrect signal that it is not a program responsibility.

CIOs also have a significant role. They must take an agency-wide strategic view of implementation and ensure that the security of each program is appropriately consistent and integrated into the agency's overall program and enterprise architecture.

-- For evaluation, the Security Act requires program officials and CIOs to annually look at what they have done and what they believe remains to be done and for IGs to verify it.

OMB's Security Role and Current Activities

Working within the above legal framework, OMB's goal is to continuously improve Federal agency security programs. Our guidance:

-- ensures that agency senior managers devote greater attention to security;

-- requires agencies to tie security to their capital planning and investment control process and to their budgets as required by the Clinger-Cohen Act, the Security Act, and OMB policy;

-- helps agencies achieve consensus and get user buy-in when initially establishing security controls and processes to ensure that they enable and do not unnecessarily impede business operations;

-- requires that security is part of agency program management decision making -- to connect the dots from security to mission; and

-- makes adequate security a condition for the funding of each capital asset by requiring that security controls and their costs be explicitly identified in the life cycle planning for each system and program.

As you may have discerned from the agency security report submissions, the agencies have reported that for FY 2002 they were investing approximately $2.7 billion for security and critical infrastructure protection. This is from a total information technology budget of about $45 billion. But a high dollar figure says little about how effective security might be, so we are working hard to ensure that these resources are applied wisely for both security and information technology in general.

To ensure that security is addressed both in the apportionment of FY 2002 agency funding and in their FY 2003 budget requests, OMB has established the following four criteria:

-- Agencies must report security costs for each major and significant IT systems. Systems that fail to document security costs will not be funded.

-- Agencies must document in their capital asset plans that adequate security controls have been incorporated into the life cycle planning and funding of each system.

-- Agency security reports and corrective action plans are presumed to reflect the agency's security priorities and thus will be a central tool for OMB in prioritizing funding for systems.

-- Agencies must tie their corrective action plans for a system directly to the capital asset plan for that system.

Government Information Security Reform Act Reporting

In September we began receiving the annual reports, required by the Security Act, from agencies. We are reviewing them now; because we know that there will be much consultation with the agencies regarding their submissions, it is too early to provide any specific findings regarding any particular agencies. We have provided you with the raw agency executive summaries and trust you find them useful, as you know they represent but one piece of the overall puzzle we are trying to assemble. Later, I will provide you some broad observations, but first I want to discuss our process and how we have gone significantly further than the law requires insofar as reporting and follow up are concerned.

As you know, the Security Act's reporting requirement is relatively narrow, i.e., each agency Inspector General (IG) must perform an annual independent evaluation of the agency security program, the agencies then send these to OMB, and we are to prepare a summary report to Congress.

Because security is a high priority for this Administration, we have expanded the Security Act's limited requirement. OMB first issued guidance on implementing the Security Act in January. This guidance clarified the roles and responsibilities of CIOs, program officials, IGs, and OMB responsibilities. Additionally, the guidance required agencies to prepare an executive summary consisting of two components, an IG and a CIO part, based on the results of their respective reviews.

Follow-up OMB guidance issued in June contained detailed instructions to agencies on how to report their results in the executive summaries. These executive summaries will serve as the basis for the OMB annual report to Congress. We have also required that agencies send to us sufficient documentation that supports their findings in the executive summary (the Security Act requires agencies to prepare reviews but not report them).

To ensure that this reporting does not devolve into a bureaucratic paper drill, we are also requiring that agencies produce for their own use and send to us copies of corrective plans of action and milestones for each weakness found by an IG evaluation, a program review, or any other review conducted throughout the year, including a GAO audit. OMB issued specific guidance for preparing and submitting these corrective action plans and provided a template to assist agencies in developing them. These plans are not just important to us, but to the agencies and IGs as well. They bring a discipline to the process and make tracking progress much easier for all involved. We will also seek brief quarterly certifications that corrective actions are on track.

We haven't stopped there. We are requiring that each of the agency program reviews (which should also include individual system reviews) and plans of action are tied to the budget process through the corresponding capital asset plan and justification submitted with the agencies' budget. In this way, we ensure that funding requirements for correcting the weaknesses identified in the plan of action are accounted for in the agency's funding for an asset. As I said earlier, unless security is incorporated into and funded as part of each investment, the investment itself isn't funded.

Finally, we intend to use the security reports from the agencies, information we have gathered from meetings with the agencies on integrating security into their capital planning processes, their budget submissions, and other sources to determine whether OMB must take steps to assist agencies in quickly correcting their most serious weaknesses.

Overview of Agency Annual Security Reports

In their security reports, agencies reported $2.7 billion in security costs for FY 2002. Despite this sizable investment and the fact that law and long-standing OMB policy give agencies extensive flexibility in implementing security in a way that comports with their operational realities, there still remain significant security concerns across the government. We do not believe that, again given the large total amount already being spent on security, that simply adding more money will solve the problems. Such an approach has not worked for IT in general -- it shifts attention away from effective management and investment of existing resources - and will not work for IT security.

Generally, from agency security reports, especially the work performed by the Inspectors General, we have found across the 24 CIO agencies that the most common problems involve inadequate compliance with existing OMB security policies and failure to follow implementing guidance for the Security Act. From our preliminary findings agencies must:

-- Do a much better job testing and evaluating basic security controls;

-- Improve the ongoing maintenance of system security;

-- Greatly improve employee training and awareness programs;

-- Do a better job at integrating security into the capital planning and investment control and budget processes to develop a better understanding of security costs and ensure that security is in the program planning mainstream;

-- Recognize the greatly increased risk of interconnection;

-- Ensure that every system supporting operations and assets are reviewed annually as part of a program review; and

-- Pick the low hanging fruit by installing readily available patches for commonly known vulnerabilities. This is a chronic problem identified by GAO, IGs, and most any security program review. It is also commonly reported from FedCIRC and others as the cause of some 90% of successful attacks on agency.

Recognizing that this is the first year for these reports, we have to expect incompleteness and inconsistency, but we will work with the agencies to ensure that any incomplete submissions are corrected and that each agency fulfills their security responsibilities and meets the specific requirements of the Security Act and OMB guidance.

Security and Electronic Government

We have also taken steps to ensure security is a key component of other OMB activities. The Administration's E-gov Task Force identified and the President's Management Council approved 23 cross-agency e-gov initiatives. OMB, working with agencies, will refocus resources to assure that IT facilitates agency administrative efficiencies, and most importantly, maximizes citizen access. In the process of making government easier, quicker, cheaper, and more responsive we must also make sure that government and its information and services are adequately secure.

All of the e-gov initiatives must address security. In addition to a risk management plan, agencies must demonstrate for each initiative that security for the initiative has been assessed, appropriate security controls identified, and that the agency has a process in place to maintain effective security for the project over its life cycle. In addition, three of the e-gov initiatives specifically deal with security issues:

-- E-authentication: Ensuring that parties to a transaction are authorized to participate and ensuring the integrity of the transaction.

-- Wireless Networks: Ensuring effective and interoperable communications between public safety officials throughout all levels of government, before, during, and after their response to a variety of events, such as natural and technological disasters, terrorist actions, and criminal activities, as well as to conduct other life-saving activities such as search and rescue operations.

-- Disaster Assistance and Crisis Response: Providing a one-stop portal containing information from all public and private organizations involved in disaster preparedness, response, and recovery. It will address the consequences of a disaster whether natural or man-made, technical or physical.

Security, the Government-wide Architecture, and Project Matrix

As a central part of our e-gov efforts we are developing a government-wide enterprise architecture. Establishment of an architecture for the Federal government will greatly facilitate information sharing based on the lines of business of each agency. Additionally, this architecture will identify redundant capabilities and provide ample opportunities to increase efficiencies while reducing costs, and duplicative programs. Accordingly, we will also be able to better prioritize and fund our security needs.

A significant piece of this effort is the identification of key critical assets. Unlike the larger general security program, identifying critical assets and their interrelationships is especially complex and time consuming. The Critical Infrastructure Assurance Office of the Department of Commerce has developed a critical asset identification program known as Project Matrix. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships within the agency and beyond -- the enterprise architecture. Project Matrix reviews have been conducted or have begun at nine large Federal agencies. OMB is directing most remaining large agencies to reallocate FY 2002 funds for a Matrix review. To ensure that all critical government processes and assets have been identified, once reviews have been completed at each large agency, OMB will identify cross-government activities and lines of business for Matrix reviews. In this way we will have identified both vertically and horizontally the critical operations and assets of the government and their relationships beyond government -- the government's critical enterprise architecture.

Conclusion

The security problems found throughout the agency reports are not new. We have established a focused, cross-agency approach to address this serious issue. Building on the framework established in the Security Act, we are requiring agencies to document their work in corrective action plans to ensure that security problems are prioritized and resolved in a timely manner. Additionally, we have taken steps to further integrate these security activities into the budget process. Clearly, sustained senior management attention at the agencies is essential to ensure the success of these efforts.

We plan to engage the agencies in a variety of ways to address the problems that have been identified, we will be emphasizing both the responsibilities and performance of agency employees in addition to accountability for exercising those responsibilities and consequences for poor performance.

We are going to stop funding for any project that does not adequately address security requirements and neglects to document how security planning and funding is integrated into the life cycle of the project.

At the same time we are going to focus on achieving sustained senior management attention at the agencies. This has been a chronic problem that we, GAO and others have found over the years to be the underlying cause of poor security performance. Indeed GAO's 1998 Executive Guide to Information Security Management identified senior management attention as a key to security success at leading organizations.

In discharging our responsibilities under the Security Act, the Director will be communicating with the appropriate agency heads to impress upon them that true improvements in security performance comes not from external oversight from OMB, IGs, GAO, or Congressional Committees, but from within - holding agency employees, including CIOs and program officials, accountable for fulfilling their responsibilities under the Security Act. There must be consequences for inadequate performance. We will also underscore an essential companion to that accountability -- the clear and unambiguous authority to exercise the responsibilities.

Despite the security challenges we face, we are not delaying our aggressive move towards accomplishing the President's Management Agenda including using secure information technology to make government more effective, responsive, and citizen centric. We can and will accomplish our goals.

I want to thank you and the Committee for your help and continued focus on this important area. It is vital that we all work together to maintain this as a priority issue and thus promote a more secure government.

Mr. HORN. Thank you, Mr. Forman. Both you and Mr. Dacey have fine careers in the private sector as well as the public sector, and I guess I would ask you if you looked at these charts and the subcommittees charts, what would you do if you were still in the private sector?

Mr. FORMAN. Well, I have two——

Mr. HORN. Would there be a new computer director?

Mr. FORMAN. I have two views on this. No. 1, I would and I will, as well as the Director of OMB, use your data and our data in communications as part of the 2003 budget process. That will go back to the hill.

And as I indicated in our testimony, we have authorities on the apportionment of funds in 2002. I think we have made clear that we're not going to fund systems that don't meet the requirement of what we require to be a valid business case, and computer security at the heart of that.

The second thing that I think we all need to be cognizant of, the reports, as I read the evaluation, are based on valuation of agency reports, you know, whether from the IGs and GAO, or from the agency themselves. And I don't believe we have the data that we need into the details, so if I go into a server form or a data center have they been pulling down, for example, the IIS patches that they need to deal with Red Worm? We put out a call via FedCIRC to get the CIOs to ensure that indeed this was occurring. And what we found out is, yes, it had occurred. There were no issues in many of the agencies. What we found out in some other agencies, this was not on the platter of some of the CIOs. So when we get into the details I think we are going to find a mixed bag, and I think that is where we need to go over this next year.

Mr. HORN. Mr. Dacey, you have a similar career in the private and public sector. What would you do if you had this bunch of grades dumped on your desk some morning?

Mr. DACEY. Well, I think the first step is along the lines of what Mark had said. I think you really need to take an assessment of really how bad or good is your security, what's working good and what's working bad. Since we started doing work probably in 1996, generally in connection with the CFO Act and other congressional requests, we have gained a lot more information as the years have gone on and continued to find significant weaknesses in computer systems. But I don't think that we have an end-all analysis at the type of detail level that Mark referred to.

So I would suggest the first thing to do which is contemplated by the GISRA legislation is to go out and ensure that you really understand the nature of those vulnerabilities and weaknesses. I think, again, that needs to be done. We have not had time to really analyze the GISRA reports to see how much additional work has been completed beyond what was done before GISRA. But I think that is an important area.

Second, I think it is important to realize that what needs to be incorporated is really an acknowledgment that computer security is part of your basic operations. It's really a responsibility of everyone in the agency, and you really need to put in place reasonable and adequate computer security management programs to ensure that. I think it is very important for management to have some regular analysis of their systems as well in order to manage and maintain some level of accountability and performance measurement. I think those are important aspects of the GISRA legislation as well because we do have an annual accounting now, at least for the 2 years that the law currently covers, to address that issue, and then, given the identification of these weaknesses, really setup a very active plan to address them, including looking at ways to benefit from what is being done across other agencies.

What I see now a lot is each agency trying to address their computer security, setting up what they believe to be an adequate security process. Even within agencies, bureaus within agencies are setting up sometimes vastly different levels of security based upon their judgments. I think there needs to be a coalescing of some of that information, establishment of some common level of controls, at least a baseline, to tell people here's what you really need to have, and not have each agency try to figure out on their own how they get to that point in time. Those are the kind of things I think I would suggest from a private sector approach to try to address a problem of this magnitude.

Mr. HORN. The chief information officers have a council, and they have subcommittees and committees within that council. Are you both members of that, or at least Mr. Forman for the administration?

Mr. FORMAN. I serve as the director for the council.

Mr. HORN. Yeah. Now, do you think they take this seriously, or is this just regarded by either OMB or this subcommittee that they say, oh, just another piece of paper we've got to fill out; how are we going to solve that problem and get them involved to really know it's serious?

Mr. FORMAN. I think that they do take this seriously. As you know, we have reorganized the council and haven't completely finished the deployment of that. Security is one of the areas that we are working through a number of options. But we have chosen to disband for now the Security Committee, and I think it is important to understand why. We've got a good best practices guide out of that committee. We had many members on that committee who are in key agencies. We do not see any correlation based on the data between membership on that committee and either your scores or our scores of success. We need to get into the nitty-gritty details.

We have a Work Force Committee. There are two key elements of the workforce that we and the CIOs need insight on. No. 1, what are the standards of performance for security personnel? What types of skills should we be looking at, both in terms of who we're hiring and who are in those positions within the government. And I'm forever cognizant of the fact that 80 percent of our IT work force is through contractors. So what are the basic skills and capabilities we need? We need more insight on that and then we need to hold the agencies accountable. That task was given to the Work Force Committee.

The second type of work force skills, Web masters, Web designers, virtually everybody, every career field in IT, now has some aspect of security. So clarifying those responsibilities, those knowledge requirements and skill requirements, is the other thing that the Work Force Committee is doing.

The Best Practices Committee will continue to focus on best practices. We have chosen to give National Institute for Standards and Technology a higher role in this arena as a source not only of the Federal information processing standards, but also a terrific source of best practices.

The third area in this is the architecture area. We have an Architecture Committee. We have to get agreement among the CIOs of some of the common best practices as they relate directly to the architectural elements. So it is my intent to force that debate and that consensus building that we need via that committee.

Now we are looking at how do we best drive the cross-cut across all the CIO agencies. And to date, quite frankly, I've been fighting the maintenance of a committee just to talk about this, because we do not see that correlation between committee membership and success.

With that said, we have some other options. Do we appoint a couple of people, CIOs that basically marshal across the other standing committees to focus on security and ensure that it's getting out to all the other CIOs? We had a roundtable discussion a couple of weeks ago, a 2-hour discussion where the CIOs to a "T" were either there in person or there with their deputy CIO. So I believe they are very focused on this issue. And we have a 5-page list of ideas we need to focus on and alternative ways to handle that. We are pulling that material together now. We will have another meeting and discussion of this at the CIO Council coming up next month to make some choices on how we'll proceed.

Mr. HORN. Were you at OMB when the argument—I don't know whether you have it an argument or what—between the council and OMB as to what kind of questions ought to be used to look at what the hardware and software are with these computer operations? And were you there when this particular group—and this grading thing we have done is really just look at what OMB did, send out to 24 of the major agencies and departments, and that's all we did. Do you think we have been unfair in reaction to these grades?

Mr. FORMAN. I am not quite sure I understand the question, but let me try.

Mr. HORN. Well, were you around when this particular inventory, let's say, was sent out by OMB, and we simply—and GAO—simply said OK, they put the questions to them and let's see if it works?

Mr. FORMAN. It actually occurred just before I came on board, the original criteria were sent out.

Mr. HORN. So you're innocent so far.

Mr. FORMAN. No. Hold me accountable. Let me give you my view on this.

Mr. HORN. Yeah.

Mr. FORMAN. Accountability and authority go hand-in-hand for me. If you hold me accountable, I have a way to hold the agency accountable.

Mr. HORN. Good. We'll do that. Maybe we'll see you a few months from now. And one of my friends in the Cabinet on the Y2K thing simply took our grades and put it on his door, so every time a civil servant went in to see him, that grade was right in their face. And he said it helped, a little bit of—that grading got them moving. So what else can we do? What else can you do? You're the one now on the frying pan.

Mr. FORMAN. As I mentioned, in preparation of the fiscal year 2003 budget, we have got some rather strong action that we intend to take as part of the past act, discussions that I hope will lead to reconciliation of gaps that we see and will address, some of the poor grades that you see as part of the 2003 budget submission. You will see that result, I hope, coming back very well in the President's budget submission.

Second, as I mentioned, we intend to use the Clinger-Cohen Act authorities on basically the apportionment process. So what I would ask is your cooperation, because I am sure that there may be other agencies or vendors that come to the Hill and talk about how unfair that is. That will take persistence and backbone by all of us to be true to these ideals.

Mr. HORN. How would the government have fared if, on September 11th, a cyberattack accompanied the physical attacks on the Nation? Would that have got them moving on such things as security? Or is it just, as I said earlier, well, let's see the paper, OMB. We have been around here a long time and it's the same old game. So what do you think?

Mr. FORMAN. I think things have clearly shifted, and I would daresay that it may not be as press-worthy. But if you look at the worms that came out this summer, that our battle in the computer security arena really started in perhaps the July timeframe when the first of the worms started to hit. So I know from OMB's standpoint all the way up to the director, this is, believe it or not, the type of thing that we would talk about at these staff meetings. We are very focused on this. And it started in July.

Mr. HORN. Well, when you provide us with examples of agencies whose requests will not be funded because they've failed to document their security costs, that would be an example of getting their attention. Is that what you're planning to do?

Mr. FORMAN. Well, we hope that we will be able to——

Mr. HORN. Or are you being Mr. Nice Guy?

Mr. FORMAN. At some point, I'm sure that I'll appreciate the time when somebody calls me Mr. Nice Guy, after we go through this budget process. We hope that based on the feedback that we're giving to the agencies and will continue to give with the agency in preparation for the 2003 budget, that we will reconcile these issues. Obviously, if we are unable to reconcile the issues, that list will be in the budget.

Mr. HORN. Do you agree with GAO's recommendation to establish mandatory standards for Federal agencies?

Mr. FORMAN. I think it is a question of the details on the standards. I think we have laid out some fairly clear standards in both the requirements for the government information Security Act reporting and within the guidelines of what we put into my testimony. I think a little bit more specific standards. The standards that we have been promulgating along the lines of how do you hold the agency accountable and link that to funding are actually in both A–130 and the A–11, our basic budget documentation. So I think that is consistent with what GAO is proposing.

I actually think there is another set of standards that get down to the real technology. When do certain data elements have to have a security wrapper, which with XML technology is currently available. When do certain elements of transactions or certain uses of virtual private networks have to have encryption or other types of security? It's those standards that I want to get the agreement via the CIO Council Architecture Committee, and that is the process I would like to pursue for buy-in purposes.

Mr. HORN. Mr. Dacey, let me ask you on the September 11th question, how would the government have fared if on September 11th a cyberattack accompanied the physical attacks on the Nation? How would GAO feel about that?

Mr. DACEY. Well it's difficult to speculate what would have happened. I know on the physical side we had disruptions in communications and other areas. Fortunately at this point in time, we haven't suffered from disastrous effects of a cyberattack. As in our testimony we stated, though, there are signs that things are getting more serious, more sophisticated, that it could really be a serious issue. Particularly when you look at how dependent we, the Federal Government, are on computer technology and communications channels being available to do our business on a day-to-bay basis. So I think when you look at those things, you have to start analyzing what could go wrong.

And in terms of the critical infrastructure, I think that's one of the areas that Mr. Forman refers to needs attention and has been given attention, and, through Project Matrix, has really had to identify what those critical areas are so they be protected adequately; at least focus the priority on protecting those first to ensure they are protected.

But I think that is an exercise that needs to be done, certainly in the Federal Government. And then as part of the overall CIP structure, consideration of what needs to be done or what is being done in the private sector. There's a private sector partnership here, because a lot of the critical infrastructures that even the Federal Government depends on for communication, electricity, and others are all controlled by the private sector, mostly controlled by private sector interests. So I think it is important that those be dealt with, too.

So I think we have, certainly, challenges ahead of us to make sure our systems are secure before something happens that is more disastrous. Again, we've had a lot of attacks, it's cost a lot of money; I don't want to diminish the fact that they haven't been serious, because they have. A lot of productivity, a lot of money has been lost. We had the testimony before this committee out in California in the field hearing and talked a little bit more about that along with the other witnesses, but I think it is an issue that just needs to be addressed now; and again in an organized fashion, not to say that it isn't, but it needs to go forward, again, with really a strategic plan. And I think some of those things we're starting to see at this point in time.

Mr. HORN. Well, the General Accounting Office has been reporting on many security weaknesses in the Federal systems for—as your testimony just notes—Federal systems for several years. Yet based on today's grades, agencies don't appear to be making any progress in strengthening their security. Do you agree?

Mr. DACEY. Well, I think we are seeing not necessarily every agency, but many are making some significant progress in improving security. We talked about a couple of those certainly. We had the issue to report earlier this year on the electronic filing system, and IRS had taken extreme efforts to make sure that was secure for this last filing season. We have had a lot of improvement to the Department of Defense as well, although they continue to face challenges in putting together a security management program, they do have some of the basic elements in place at this point in time. So there have been improvements. What is really challenging I think in this environment is that the pace of these risks is increasing extremely rapidly. Some of the factors that make it more of a risk are increasing at a fast pace, so we are not dealing with a static target that we need to hit. I think the target's moving perhaps more quickly than we are at this point. I'm not saying it is, but I'm just saying that's the challenge to keep up with that.

So I think in terms of perspective, again, a lot has happened. Probably if you want to secure the systems, the pace may need to be stepped up a bit from what it has been to catch up.

Mr. HORN. Do you feel any of these grades are being easy on people or being too tough on people? What's your thinking on that?

Mr. FORMAN. I'm concerned just about some of the discrepancies. You have a couple of grades that are easier than ours. We're going to hold the agencies accountable, I think, for the harder grades in those cases. The Defense Department is the big gap that we see between our grades and where you graded it harder than we have. I suspect that is because they came over and presented much more material to us than your staffs had access to. You know, I don't know that would change necessarily the grades that you give them. But that would be the only discrepancy, major discrepancy I would say.

Mr. HORN. Which grades would be easier?

Mr. FORMAN. I'm probably not willing to get into that at this point. We're going to reserve that for the directors' communications with the agency heads.

Mr. HORN. So you've got sort of several professors down there that are putting different kinds of grading or what? Or can you agree on what an F means or an A means? Or is this the 60's, anybody down there in the 60's? Because if there are, you know, what the heck, it's just give everybody pass/fail.

Mr. FORMAN. No, there aren't that many discrepancies. There are very few discrepancies. Please let me leave it at that.

Mr. HORN. OK. We'll see what happens in about 2 or 3 months from now, see if we've made some real progress. And I am curious, Mr. Forman, while I understand the government information security reform requirements do not establish a date by which OMB must submit its required reports to Congress, when will OMB submit this report?

Mr. FORMAN. Our intent is to submit it with the budget. If it is not with the budget, it will be very near to that submission. And of course that goes along with the basic enforcement mechanism that we are pursuing.

Mr. HORN. Well, that's—I'm glad to hear because we were wondering where that was. You're OMB's associate director for IT and E-Government, don't agencies' security weaknesses as indicated by the deplorable grades we assigned today, post a formidable obstacle to implementing more E-Government initiatives? How does OMB and E-Government strategy explicitly address computer security? Are we on the wrong thing, or how much of that, if you will look at all of the inventory and the form, that was sent out by OMB, is this a 5 percent or is it a 25 percent? Do they take it—how do they take it? That's what I'm after, in terms of percentage, that they worry about and try to do something about.

Mr. FORMAN. Well, I think for each of the E-Government initiatives it is a 100 percent, because we made very clear that we are going to use the A–11 guidance in putting together the business case for each of these E-Government initiatives. In doing the work of our quicksilver task force, our E-Government strategy team, we identified several cross-cutting barriers. Of course, as you would anticipate and as you pointed out, there are a number of security-related items that came out of that. And indeed, that is this E-authentication initiative that we've begun. That's going to have a business case as well. Now, we have included that in any one of the customer segments, the bulk of our initiatives focus on a customer segment government, citizen government, and business etc. The security initiative is a cross-cutting initiative. It relates to agency-to-agency or within-agency transactions as well as interactions between Federal, State and local governments, governments and businesses, and government and citizens.

That business case, as all the business cases, will have to report not just to me but to a steering group. The steering group will in most of the initiatives be comprised of the different management councils, CIO Council, etc. In this case, the steering group we're going to use is that Architecture Committee of the CIO Council. So when we come to resolution on authentication and digital signature and E-signature elements, which we found is the most critical element for the E-Government initiatives, that agreement has to get the support of all of the CIOs because it has to be embedded across the department and agencies.

There is another infrastructure issue that came out of the task force, which basically I refer to as the business architecture analysis. And integrating that with the Project Matrix data at each department as we look across the business architecture, all the agency-to-agency interactions, is another level of analysis that we'll continue to do coming out of the task force.

Mr. HORN. Let me ask Mr. Dacey. In your testimony, you state the number of incidents are increasing, yet one agency, OPM, reported that during the past year it only experienced one security incident which involved limited infection by the "I Love You" virus. How do you react to this statement?

Mr. DACEY. Well, I think one of the challenges that we have is twofold. First of all, one of the basic premises on security is to have the first adequate level of security in place, particularly at your perimeters, for people to get into your systems, but security, as good as it can be, is never going to be foolproof. So there is always going to be opportunities for people to breach that, even in a good security situation.

So you really need to have effective incident detection processes in place to identify when that has happened and to really identify unusual or anomalous activities. I think what we are finding, both in the Federal agencies as well as the challenge in the private sector, is the identification of that type of intrusion. I know one of the parts of the GISRA legislation is that agencies have effective incident detection systems in place. In working and discussing things with the CERT Coordination Center, which is funded heavily by the Federal Government and receives a lot of information from both private and public sector in terms of incidents, they said their information indicates that as many as 80 percent of incidents are not detected, and that is across the board. So I think we have a tremendous challenge. That is in fact one of the areas that research and development could really help to identify better techniques, because we do have a ways to go to really develop more effective mechanisms to identify those.

The volume of scans and activities coming into any agency is phenomenal. We have a rather small laboratory that we use to help do the work that we do. We've gotten 3 million or so scans of our system within 3 years, and that is something that is not well advertised, even our address. I know even at home personally, when I go online, my firewall is picking up three or four incidents an hour of someone trying to get access to my system. So activity is happening out there. We just need to have a better system to figure out what is valid and what is not valid in those systems, and it is going to be a challenge.

Mr. HORN. Along this line, the subcommittee based its grades on information submitted to OMB by the agency CIOs and IGs in their reports on the annual agency security program reviews required by the Government Information Security Reform Act passed last year as part of the fiscal year 2000 Defense Authorization Act.

Now, how do you account for the substantial discrepancies that we noted in several cases between the CIOs report and those of the Inspectors General? Are some agencies' CIOs underreporting their vulnerabilities?

Mr. DACEY. Well, I think one of the challenges as part of this process—again, not having fully analyzed what was reported—is to really get in place a mechanism whereby there can be some agreement on whether the security controls are effective or not. What we have seen in the past is that a lot of the analysis and actual testing of those systems is being done by the Inspectors General, and although we note some activity by managers actually testing their own systems, we haven't seen a lot of that happening to date. So what I think you have oftentimes are situations where the ID is actually going out as we do, trying to break into systems, trying to really analyze those controls, and I think what we need to do, which has started to happen with GISRA, is say, managers—program managers, you're the ones responsible for security. It's not the GAO or the IG coming in every once in a while and doing a testing of this system or that system. Management really needs to put in place procedures and processes to monitor their own systems on an ongoing basis regularly, which, again, GISRA facilitates that through annual reporting processes.

So I think there are bound to be some difference, at least initially. I would hope that over time, though, that if the agency manages to actively test their own system, which is a very important piece of the legislation, that they will find similar types of weaknesses, and you'll reach some conversions. There's always going to be some differences in judgment, of course, but I think overall that is the biggest difference now, is the methods by which maybe that management was obtained. A lot of this information from the management side may have been through just various means, assessments, questions that went out to the field and talked about whether the security is adequate and what they have done. I don't know.

Mark may be able to shed some more light, because we haven't been privy to all the detailed information, but again, that would be one potential area as to why there are some differences and how those two might converge in the future.

Mr. HORN. When we went through the Y2K situation, Mr. Koskinen was the Deputy Director for Management. Nothing much happened, and he retired, and then the President very well called him back, and he was a friend of the President's, and much like Governor Ridge, that—he's got Mr. Clarke, a lot of respect for both the Governor and Mr. Clarke on these matters. If I were a Deputy Secretary or something, I'd sure want to please him. So the question is, is he the Lone Ranger that comes in across the prairie and you guys are just waiting for him to do your jobs? How do they think about that at OMB?

Mr. FORMAN. First of all, in both Executive orders, it is very clear that OMB maintains its role for the oversight and management, if you will, of agency security. So while we're disbanding the CIOs Council Security Committee, under the Executive order in the Critical Infrastructure Protection Board, OMB does chair a security committee that has been created for Federal infrastructure. So the linkage and the working relationship will be very good, I think.

Not at all would I say that we're going to toss our responsibility up the hill. This will be another area where we hope to be held accountable for the work, but I want to build on something that Mr. Dacey said. You know, when we look at this, ultimately it's got to be built into—we've got to have security built into the actual programs. GAO several years ago laid out how do you manage capital investments in general. Our focus on the business case process is, I believe, the appropriate focus that we should move forward. So in the capital planning process, the first step is make sure security is part of the business case, and that is essentially the phase that we're in now in driving into the agencies. I think by us saying we're simply not going to fund the business case that does not incorporate the appropriate security controls, complies with that first phase of GAO's three-part practice.

The next phase is the actual program control. Is it actually being built in? Are the agencies and are the program managers working on the security components or modules as they execute that program? The third phase is the followup, and it is not just lessons learned and best practices. I think that's exactly as Mr. Dacey has said, we've got to have the affirmative testing, that in fact the security is break-proof at that point.

The difficulty is every time you move forward in preventative approaches for security, the hackers move forward in a way to break through that. So we're dealing a little bit with the moving target. We have to make sure that is integrated and updated, and I'm a big fan of maintaining the business cases and controls over those business cases. So I believe that the approach that's been laid out for capital investment management is the same that we should be employing here.

Mr. HORN. Are you seeing any changes or new computer security initiatives within the agencies since September 11th?

Mr. FORMAN. Absolutely. We have much help from our friends on the Hill. As you know, we have at least one bill suggesting that we spend $1 billion more on computer security. We appreciate the cooperation and the focus on security. Clearly, more money is not the issue. Focus is, and the details, as I think you've focused on in your scores where we need to look.

Mr. HORN. And you're saying how much do you think you can get out of them this time? Because I went around last year with the number of things the executive branch wanted, and some of them got it and some of them didn't. It was a little haphazard. So it is nice for OMB and you to get it moving. And how much do you think you can get from them?

Mr. FORMAN. In terms of focus on this, I have to say based on the reports that have been submitted—and, again, I'm quite impressed with this—this is the first time that I have seen Secretary level or agency head level focus on this issue. And so I think that occurred before September 11th. This was—the reports came in September 10th, and it's just I think after that become all the more important and it's recognized. I hope we get full compliance by the Secretaries. Our intent is in the process between now and the final submanagers of the budget, that we will have that communication at the level of the OMB Director to the Secretaries of the agencies.

Mr. HORN. Mr. Forman, we discussed that OMB and CIOs and IGs and their reports, and that those were required by the Government Information Security Reform Act passed last year as part of the fiscal year 2000 Defense Authorization Act, and I'd like it on the record, is OMB satisfied with the quality of these reports and how do you account for the substantial discrepancies that we noted in several cases between the CIOs reports and those of the IGs and are some agency CIOs underreporting their vulnerabilities?

Mr. FORMAN. When you say are we satisfied with the quality of the reports, are we satisfied with the quality of the content or the completeness of the reports, I guess would be my question? I think that in both cases, we'd say we're not fully satisfied. So let me explain that a little bit. This is the best set of information that we've had so far going back to 1987 in the Computer Security Act on agency assessments. We want more. That's the bottom line.

In some cases, the agencies have come back afterwards and provided us the additional information, in many cases. Are we satisfied with the content? There are clear examples of dramatic progress versus the information that we had received before. I would say that the high—areas where you have given agencies higher grades are not an area where we are seeing any of the agencies. So my answer would be, as has been said before I believe before this committee, I don't do C work. I don't want the agencies to do C work. I'm not satisfied.

Mr. HORN. Good. Glad to hear it. How long will it take you to turn them around?

Mr. FORMAN. I don't know the answer to that. I'd like to be able to come before you a year from now and to say that we've got a substantial amount of Bs. That clearly is where we'd like to go. On the other hand, as I've said before, there's another level of details associated with what we've got to get across the CIOs. The work force skills and the compliance with those skills that may not show up in the reports, the agreement on some of these security protocols and standards and so forth, that I believe is a critical element of how you should hold me accountable. But again, that won't show up in these reports. So I've got a lot to do, and I don't know if I can get to that level of B in a year from now.

Mr. HORN. To what degree does the President and OMB and all of those who see the retiring situation in the bureaucracy and how we replace it with very committed people and have understanding of the new world that they didn't come out of 20, 30 years ago? So are we going to get some incentives of getting new people into the government where we need them badly and get people to go around to the State universities in particular, I would think, and—but I'm a bias there. And those are the people that stay with it, when I looked at them in a study 30 years ago, and it still seems to be true. So what's the plan?

Mr. FORMAN. Absolutely, on the work force we're taking a number of initiatives, and, again, I'd say that these are in two prongs. One, the types of security personnel or computer security, cybersecurity personnel that we're hiring, their skill-sets, how we build their competencies and indeed the training program. The second is in a number of other job categories, Web masters, Web applications designers, the skills to do object-oriented architectures and so forth. So we have to ramp-up those skills.

Now, one point that I have to make here is that the vast majority of our work force are not Federal employees. I think we've made tremendous progress with the CIO Council Workforce Committee, under Gloria Parker and Ira Hobbs, to move forward on a curriculum. You may be familiar with the CIO university concept that basically lays out a curriculum for graduate school and related training. What we're finding is that as much or more contractor personnel are going through this course work than Federal employees. So we're making—which should be, you know, given the ratio of our work force, Federal versus contractor, we should be seeing that. We're making that progress, and I will continue to push forward in that arena.

Mr. HORN. Well, thank you very much. It's been a useful situation of going through these things, and I think 1 year is too much to wait, and we're going to have to think about it in maybe a month and a half and 2 months and a half to get, and I would hope OMB would say, get with it, and then we don't have to give Fs. So—and as you say, you don't want to have a C student there either. Often they're the ones, however, that are hiring people of a grant and what not and get rather rich in Silicon Valley.

So anyhow, we thank you for coming, and I want to thank the staff here that helped put it all together and worked with us in terms of the grading situation. Russell George, staff director and chief counsel; Bonnie Heald, the deputy staff director; Elizabeth Johnston to my left, professional staff; Darren Chidsey, professional staff, Earl Pierce, professional staff, and Jim Holmes and Fred Ephraim, interns. We're glad to have them, and on the minority side, David McMillen, professional staff; Jean Gosa, minority clerk; and our faithful court reporters are Christina Smith and Michelle Bulkley. So thank you.

And with that, we're adjourned.

[Whereupon, at 11:12 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Second

REPORT CARD

On

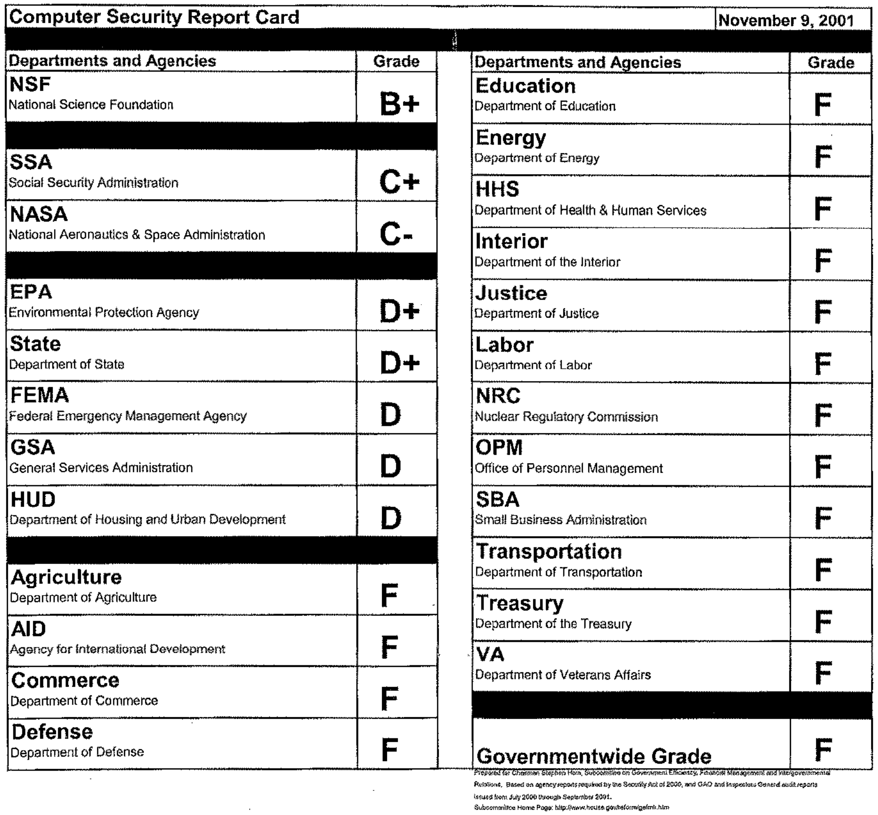
COMPUTER SECURITY

At

Federal Departments and Agencies

Overall Grade: F

November 9, 2001

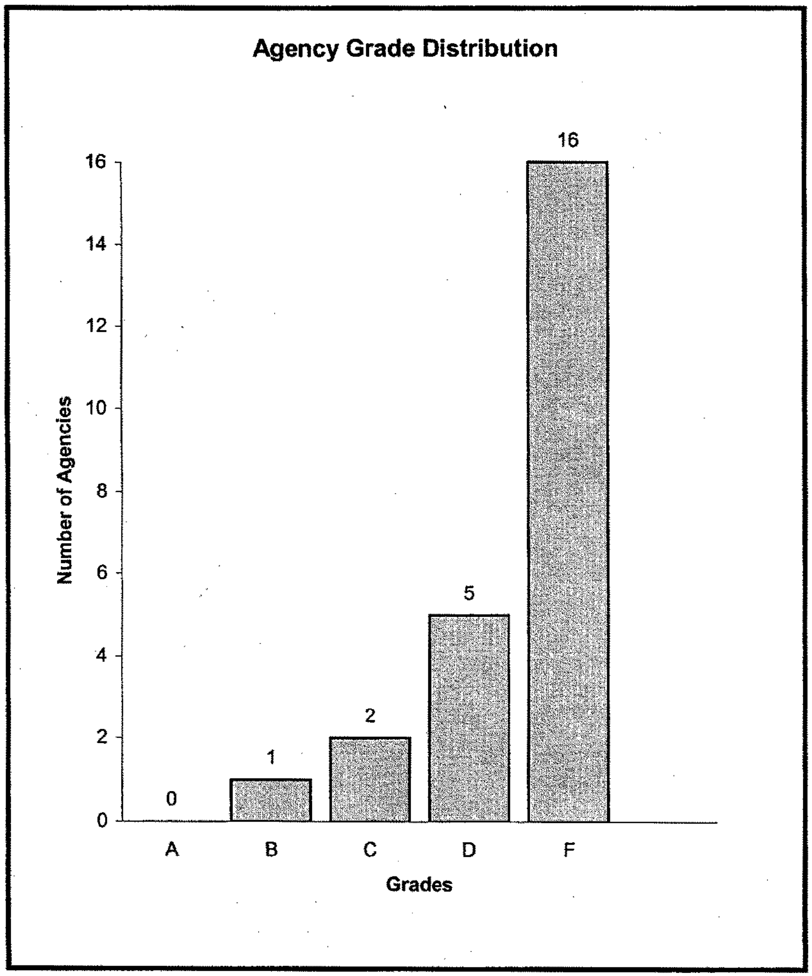


Computer Security Report Card November 9, 2001

Departments and Agencies	Grade
NSF National Science Foundation	B+
SSA Social Security Administration	C+
NASA National Aeronautics & Space Administration	C-
EPA Environmental Protection Agency	D+
State Department of State	D+
FEMA Federal Emergency Management Agency	D
GSA General Services Administration	D
HUD Department of Housing and Urban Development	D
Agriculture Department of Agriculture	F
AID Agency for International Development	F
Commerce Department of Commerce	F
Defense Department of Defense	F

Departments and Agencies	Grade
Education Department of Education	F
Energy Department of Energy	F
HHS Department of Health & Human Services	F
Interior Department of the Interior	F
Justice Department of Justice	F
Labor Department of Labor	F
NRC Nuclear Regulatory Commission	F
OPM Office of Personnel Management	F
SBA Small Business Administration	F
Transportation Department of Transportation	F
Treasury Department of the Treasury	F
VA Department of Veterans Affairs	F
Governmentwide Grade	F

Prepared for Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. Based on agency reports required by the Security Act of 2000, and GAO and Inspectors General audit reports issued from July 2000 through September 2001.
Subcommittee Home Page: http://www.house.gov/reform/gefmir.htm



Agency Grade Distribution

How Grades Were Assigned

The subcommittee's computer security grades are based on information contained in agency reports to the Office of Management and Budget, and audit work conducted by agency Inspectors General and the General Accounting Office.

Last year, the Government Information Security Reform Act of 2000 (Security Act) was signed into law as part of the FY 2001 National Defense Authorization Act (P.L. 106-398). Among its provisions, the Act requires agency Chief Information Officers (CIOs) and Inspectors General (IGs) to evaluate their agency's computer security programs and report the results of those evaluations to the Office of Management and Budget (OMB) in September of each year.

In June 2001, the OMB issued reporting guidance to agencies on implementing the Security Act, directing them to transmit copies of the annual agency program reviews, the IG's independent evaluations, and an executive summary. To provide a consistent format for the agency reports, the OMB outlined 10 specific topic areas that needed to be included in both the CIO and IG executive summaries. These topic areas refer to the key elements of an effective computer-security program. In grading the agencies, the subcommittee assigned weighted point values to each of these topic areas, with a perfect score totaling 100 points.

As shown in the accompanying chart, "Analysis and Scoring Criteria," maximum point values were assigned to questions according to their importance to an agency's computer security program. Since most questions provide a range of possible responses, the number of points is proportional to the extent to which the element has been implemented. For example, agencies received zero (0) points for a response of "no," more points for "partially," and the full weighted value for "yes." Based on its analysis of the CIO's and IG's responses, the subcommittee tallied the scores for the 24 agencies.

Because the level of detail and/or responsiveness of reported data was uneven, the subcommittee also considered the results of computer security audits conducted by the General Accounting Office (GAO) and agency IGs from July 2000 through September 2001 examining security weaknesses in the following categories[1]:

- **Entity-wide security program planning and management** to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

- **Access controls** to limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, or disclosure.

- **Application development and change controls** to prevent the unauthorized implementation of programs or modifications to existing programs.

- **Segregation of duties controls** to prevent one individual from controlling key aspects of computer-related operations that would allow him/her to conduct unauthorized actions or gain unauthorized access to assets or records.

[1] GAO routinely tracks the results of computer security audit work for the 24 major departments and agencies covered by the Chief Financial Officers Act. Results are shown in the accompanying chart entitled "Information Security Audit Results."

- **System software controls** to limit and monitor access to the basic operating system and sensitive files that control the computer hardware and secure the system's support applications.

- **Service continuity controls** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Significant weaknesses have been identified for all agencies in some or all of six general control categories. These weaknesses indicate the extent to which agencies have actually implemented general controls.

Points were subtracted from the agency's score for each control area where significant weaknesses have been found. Conversely, if audit work did not identify significant weaknesses in a control area, a corresponding number of points were added to the agency's score. The point values total 20 points and are distributed as follows:

- **Entity-wide security program planning and management** - 6 points;
- **Access controls** - 5 points;
- **Application development and change controls** - 2 points;
- **System software controls** - 2 points;
- **Segregation of duties controls** - 1 point; and
- **Service continuity controls** - 4 points.

Finally, some agencies have one or more control areas that have not been sufficiently audited. Because it is unknown whether significant weaknesses exist in these areas, a number of points equal to half the assigned point value was subtracted from the agency's score. An exception was made in the "separation of duties" category, where the full value of 1 was subtracted in order to prevent using fractions. The final numerical score is the result of these adjustments.

Letter grades for the 24 CFO Act agencies were assigned as follows:

90 to 100	= A
80 to 89	= B
70 to 79	= C
60 to 69	– D
59 and lower	= F

The Governmentwide grade was determined by averaging the final scores of all 24 agencies.

Analysis and Scoring Criteria

Part I – Report Grading Element	Weight (100 Points Max)
1. Does the report identify the agency's total FY02 security funding budget request broken down by operating unit and critical infrastructure protection costs? (OMB Memorandum 00-07, Memorandum 97-02, and Circular A-11)	**5 points max**
Agency provided total FY02 budget request broken down by operating unit and critical infrastructure protection costs.	(5)
Agency provided total, but not broken down by operating unit and critical infrastructure protection costs.	(3)
No specific security funding information was provided.	(0)
2. Has the agency implemented an up-to-date information security methodology for identifying and prioritizing its critical assets, including links with key external systems? (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**15 points max**
Methodology implemented, critical assets identified and ranked.	(15)
Methodology identified/developed but not fully implemented.	(10)
No.	(0)
3. Does the agency use measures of performance to ensure that program officials have: (1) assessed the risk to operations and assets under their control; (2) determined the level of security appropriate to protect such operations and assets; (3) maintained an up-to-date security plan that is practiced throughout the life cycle for each system supporting operations and assets under their control; and (4) tested and evaluated security controls? (Section 3534(a)(2) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established but not linked to any specific officials.	(8)
Performance measures are being developed, but were not implemented in 2001.	(8)
Performance measures not provided.	(0)
4. Does the agency use performance measures to ensure that the agency CIO adequately maintains an agency-wide security program, ensures the effective implementation of the program, and evaluates the performance of agency components? (Section 3534(a)(3)-(5) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established, but not specifically linked to the CIO.	(7)

Part I – Report Grading Element	Weight (100 Points Max)
Performance measures are being developed, but were not implemented in 2001.	(5)
Performance measures not provided.	(0)
5. Does the head of the agency use performance measures to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? (Section 3533(a)(1)(A)-(B), (b)(3)(C)-(D),(b)(6) and 3534(a)(C) of the Security Act)	**5 points max**
Yes.	(5)
Performance measures have been established but not specifically linked to the head of the agency.	(3)
Performance measures are being developed, but were not implemented in 2001.	(3)
Performance measures not provided.	(0)
6. Does the agency have mechanisms in place to ensure that contractor provided services or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy, and NIST guidance, national security policy, and agency policy? (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act)	**10 points max**
The agency does not have significant contractor provided services or services provided by another agency.	(10)
The agency has implemented mechanisms that provide independent assurance that 3rd party/contractor supported operations are adequately secure.	(10)
The agency has implemented mechanisms to ensure the security of 3rd party/contractor-supported operations but has taken no steps to verify that these are being implemented by the contractor.	(5)
The agency has not implemented mechanisms for gaining assurance that 3rd party/contractor-supported operations are adequately secure.	(0)
7. Are employees sufficiently trained in their security responsibilities? (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act) [Multiple responses—points awarded for each]	**15 points max**
Security awareness training provided in 2001.	(5)
Technical security-related training provided in 2001.	(5)
Total numbers of employees that received security training in 2001 provided.	(2.5)
Total cost for security training in 2001 provided.	(2.5)
8. Does the agency have documented procedures for reporting security incidents and sharing information? (Section 3534(b)(2)(F)(i)-(iii) of the Security Act)	**15 points max**

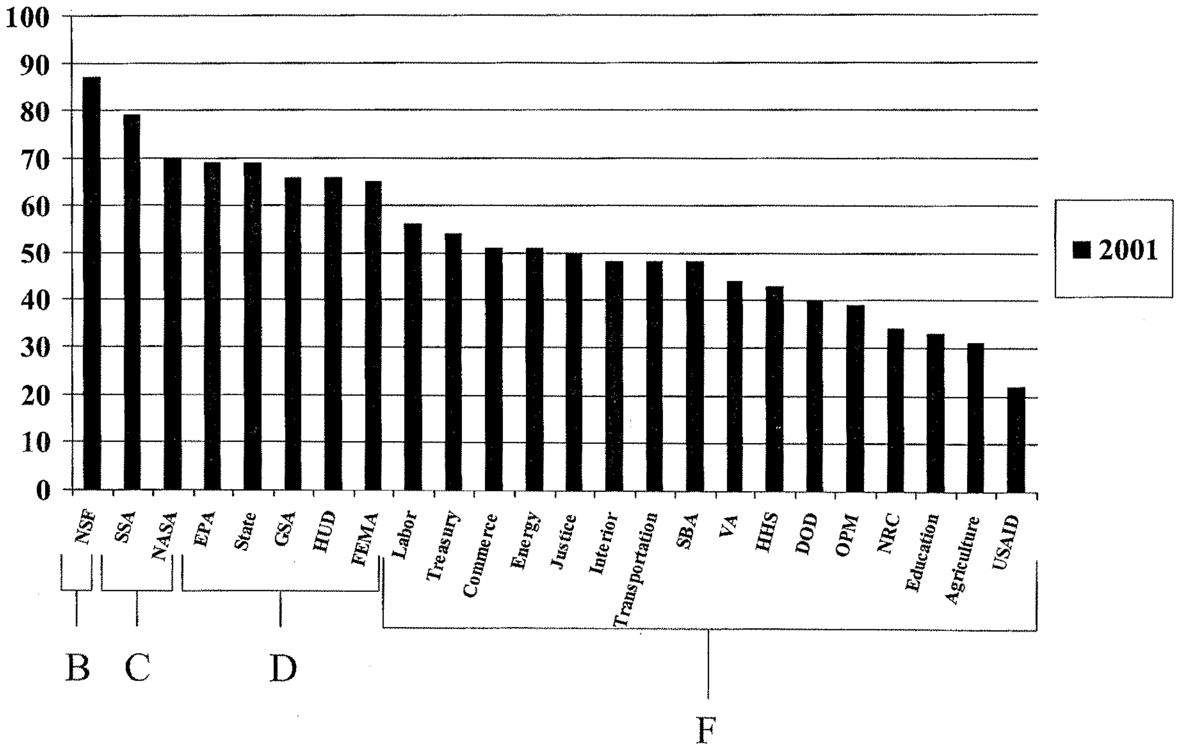
Part I – Report Grading Element	Weight (100 Points Max)
Procedures for reporting incidents and for sharing information have been fully developed and implemented.	(15)
Development of procedures for reporting incidents and for sharing information is in process or complete, but implementation is not complete.	(10)
9. Has the agency integrated security into its capital planning and investment control process? (Section 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**10 points max**
Yes, the agency has integrated security into its capital planning and investment control process and reported security costs on every FY02 capital asset plan submitted to OMB.	(10)
Partially. The agency has generally integrated security into its capital planning process but has not begun reporting security costs on every capital asset plan.	(8)
No, the agency has not integrated security into capital planning.	(0)
10. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act)	**5 points max**
The agency has no PDD-63 identified CIP systems.	(5)
Yes.	(5)
No.	(0)

Part II – Adjustment for Security Weaknesses Identified in IG & GAO Audit Reports Issued From July 2000 through September 2001	Weight (20 Points Max)
General Control Categories: Entitywide program planning and management	(±6)
Access Controls	(±5)
Application Development and Change Controls	(±2)
Segregation of Duties	(±1)
System Software	(±2)
Service Continuity	(±4)

Computer Security Grades

	2001				2000			
Agency	2001 Score Based on Agency-Reported Data	Net Adjustment for Audit Findings	2001 Score	2001 Grade	2000 Score Based on Agency-Reported Data	Net Adjustment for Audit Findings	2000 Score	2000 Grade
Agriculture	41	-10	31	**F**	62	-6	56	**F**
AID	44	-20	22	**F**	92	-20	72	**C-**
Commerce	71	-20	51	**F**	92	-20	72	**C-**
DOD	60	-20	40	**F**	89	-20	69	**D+**
Education	53	-20	33	**F**	93	-18	75	**C**
Energy	71	-20	51	**F**	98	-16	INC	**INC**
EPA	80	-11	69	**D+**	84	-20	64	**D**
FEMA	84	-19	65	**D**	77	-16	INC	**INC**
GSA	86	-20	66	**D**	81	-20	61	**D**
HHS	63	-20	43	**F**	78	-20	58	**F**
HUD	86	-20	66	**D**	93	-20	73	**C-**
Interior	68	-20	48	**F**	37	-20	17	**F**
Justice	70	-20	50	**F**	72	-20	52	**F**
Labor	76	-20	56	**F**	58	-20	38	**F**
NASA	81	-11	70	**C-**	79	-19	60	**D-**
NRC	48	-14	34	**F**	95	-13	INC	**INC**
NSF	81	+6	87	**B+**	99	-18	80	**B-**
OPM	59	-20	39	**F**	79	-20	59	**F**
SBA	64	-16	48	**F**	75	-20	55	**F**
SSA	81	-2	79	**C+**	100	-14	86	**B**
State	79	-10	69	**D+**	95	-20	75	**C**
Transportation	66	-18	48	**F**	86	-13	INC	**INC**
Treasury	74	-20	54	**F**	85	-20	65	**D**
VA	64	-20	44	**F**	85	-20	65	**D**
Federal Average				**F**				**D-**

Comparison of Computer Security Scores



Information Security Audit Results

DEPARTMENTS AND AGENCIES	QUESTION: DOES THE AGENCY HAVE SIGNIFICANT WEAKNESSES IN—					
	SECURITY PROGRAM: Plan, Implement, and Monitor Agency-wide Security Program to Manage Risk	**ACCESS CONTROL:** Limit or Detect Unauthorized Logical or Physical Access to Computer Resources	**CHANGE CONTROL:** Control Unauthorized Programs or Program Changes	**SEGREGATION OF DUTIES:** Limit Individual Responsibilities for Key Aspects of Computer-Related Operations	**SYSTEM SOFTWARE:** Limit & Monitor Access to Programs That Control Or Secure Computers and Applications	**SERVICE CONTINUITY:** Plan to Continue Critical Operations & Protect Data If Unexpected Events Occur
NSF National Science Foundation	Yes	Yes	Yes	No	No	No
SSA Social Security Administration	Yes	Yes	No	No	No	No
NASA National Aeronautics and Space Administration	Yes	Yes	?	?	Yes	No
EPA Environmental Protection Agency	Yes	Yes	?	Yes	Yes	No
State Department of State	Yes	Yes	No	No	No	Yes
FEMA Federal Emergency Management Agency	Yes	Yes	Yes	?	?	Yes
GSA General Services Administration	Yes	Yes	Yes	Yes	Yes	No
HUD Department of Housing and Urban Development	Yes	Yes	Yes	Yes	Yes	Yes
Agriculture Department of Agriculture	Yes	Yes	No	No	Yes	Yes
AID Agency for International Development	Yes	Yes	Yes	Yes	Yes	Yes
Commerce Department of Commerce	Yes	Yes	Yes	Yes	Yes	Yes
Defense Department of Defense	Yes	Yes	Yes	Yes	Yes	Yes
Education Department of Education	Yes	Yes	Yes	Yes	Yes	Yes
Energy Department of Energy	Yes	Yes	Yes	Yes	Yes	Yes
HHS Department of Health and Human Services	Yes	Yes	Yes	Yes	Yes	Yes
Interior Department of the Interior	Yes	Yes	Yes	Yes	Yes	Yes
Justice Department of Justice	Yes	Yes	Yes	Yes	Yes	Yes
Labor Department of Labor	Yes	Yes	Yes	Yes	Yes	Yes
NRC Nuclear Regulatory Commission	Yes	Yes	No	No	Yes	Yes
OPM Office of Personnel Management	Yes	Yes	Yes	No	No	Yes
SBA Small Business Administration	Yes	Yes	Yes	Yes	No	Yes
Transportation Department of Transportation	Yes	Yes	?	?	?	Yes
Treasury Department of the Treasury	Yes	Yes	Yes	Yes	Yes	Yes
VA Department of Veterans Affairs	Yes	Yes	Yes	Yes	Yes	Yes

Source: Information security audit reports issued by the General Accounting Office and agency Inspectors General from July 2000 through September 2001.

LEGEND:
Yes = Significant weaknesses have been identified.
No = No significant weaknesses have been identified.
? = Safeguards to protect computer operations and information from fraud, misuse, and disruption were either not reviewed or the scope of audit work was limited in such a way that significant agency operations were not covered.

Prepared for Subcommittee Chairman Stephen Horn
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

○